



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1430
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/688,051

10/16/2003

Ammar Rayes

50325-0800

9185

29989

7590

05/16/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER

TRAN, TONGOC

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/688,051

Applicant(s)

RAYES ET AL.

Examiner

Tongoc Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 February 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 6-18 and 21-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 6-18 and 21-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>2/7/2006</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on February 15, 2006. Claims 1, 6, 9-10, 13-16, 21, 23 and 26-28 have been amended. Claims 4-5, 19-20 have been canceled. Claims 29 and 30 have been added. Claims 1-3, 6-18 and 21-30 are pending for examination.

Response to Arguments

2. Rejection of claims 9-15 under 35 U.S.C. 101 and rejection of claims 13-14, 26-28 under 35 U.S.C. 112, second paragraph have been withdrawn in light of Applicant's amended claims.

In respect to independent amended claims 1, 16 and new claims 29, Applicant states that the cited prior art, "Proctor does not describe or suggest anything regarding to the duration of time in which a less-thorough audit and a more thorough audit are to be performed...in claim 1, the first duration of time is of a length appropriate for assessing the current activities of the user, and the second duration of time is sufficient to collect historical data regarding past malicious activities of the user (remark, page 13). Examiner notes that in cited portion of the prior art, teaches "a periodic or other time intervals, data gathered in one or more log files is collected in a data collections. A collection policy can be implemented to define the collection times or other collection parameters". This is interpreted as ***the collection of data spread in different duration of times as necessary, collection parameters are defined in the collection policy*** (see col. 6, lines 49-52). The claimed limitation may recites two set of

Art Unit: 2134

data being collected. Protor teaches the different collected information is directed to gather information about users' activities (e.g. col. 6, lines 16-20, "an audit policy may be used to define or delineate one or more users...specify operations of those users for which data should be gathered"). Therefore, Protor teaches at least one set of data (e.g. col. 2, lines 22-33, one or more instances of an actual or attempted security breach; a potential security breach; suspect; unauthorized, or abnormal activity in the networked computing environment, or out of ordinary activities or a predefined condition which may indicate a security breach or unwanted activity is being attempted). Protor teaches an on going investigation of the user or users' activities including past and present. The claimed language recites assessing a risk level of the user harming the network based on the second set of data and assessing a current alert level based on the first set of data...automatically deciding on a course of action *based on at least one of the risk level and the current alert level*. The claimed language recites a course of action in an alternative form, ***at least one of the risk level and the current alert level***. Regardless, Protor teaches "this can include ***monitoring activities to determine whether established threshold level have been met or exceed, whether activities are occurring out of nominal ranges***...If a security occurrence is detected, notification is provided to response service. Response service determines what corrective action is necessary and instructs one or more of the policy editors to update the policies...e.g. col. 14, lines 39-51. "if a security occurrence is detected, alert manager is notified...One response may be to immediately inform the agent associated with the affected target to shut down the system or to log off the user" According to the above

Art Unit: 2134

portion of the cited art, It is interpreted that Protor teaches responses to course of actions may result from risk level or current alert level. In light of this interpretation, claims 1, 16 and 29 are rejected. Dependent claims 2-3, 6-8, 17-18 and 21-22 are also rejected because by their dependency, they contain the language of the based independent claims.

In response to Applicant's remark to claims 9, contends that the cited portion of the prior art Protor (e.g. Fig. 10, 11, 13 and col. 1, line 65-col. 2, line 5 and col. 5, line 61-col. 7, line 40) does not provide any structure or functions in that correspond to the above features of claim 9. The cited claimed limitation of claim 9 recites "...receiving signals carrying network performance information regarding health of a network and resource performance information regarding to health of resources used by the network". Examiner interprets "network performance information regarding the health of the network" to be collected data pertaining to network event or occurrence that effect or hinder its normal operation and performance; "resource performance information" to be interpreted to referencing to data that pertaining to evaluation of network resource. that Protor teaches a system and method for providing enhanced security features to a computing system such as, for example, a networked computing environment...one aspect of the invention, a security policy system allows the creation and implementation of one or more security procedures. These procedures can include, for example, audit policies, collection policies, detection policies and security policies (col. 1, line 65-col. 2, line 6). In col. 2, lines 47-50, Protor further defines the definition of these policies "is usually made based on the level of security desired for the network, considering the

overhead associated with monitoring network activities and detection of security occurrence. As well known in the art, defining or projecting a level of security desired for the network encompasses performance evaluation of the network effects or hinder by event or occurrence result from security issues (or health of the network). Protor teaches monitoring or performing collection of data of user or users' activities according to set policies spreading in different time frames that results in updating these different security policies or result in immediate action such as shut down the system or logoff the user (col. 16, lines 20-26). Protor mentioned these set policies required consideration of overhead analyses (resource performance information (col. 2, lines 49-50). Protor teaches that the network procedures (include one or more security policies) are updated when information are collected and assessed (Fig. 10); each time the network procedures are updated, it is set at a different level (col. 3, lines 4-18). This meets the claimed limitation of "assessing a health level based on the network performance information and the resource performance information. Independent claims 23 and 30 are also rejected based on the similar rationale. Dependent claims 10-12, 15 and 24-25 are also rejected because by dependency, they contain the language of the independent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2134

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-12 and 15-25 rejected under 35 U.S.C. 102(e) as being anticipated by Proctor (U.S. Patent No. 6,530,024).

In respect to claims 1 and 29, Proctor discloses a policy-based network security management system, the system comprising: a security management controller comprising one or more processors; a computer-readable medium carrying one or more sequences of instructions for policy-based network security management, wherein execution of the one or more sequences of instructions by the one or more processors causes the one or more processors to perform the steps of (see Abstract):

receiving a set of data regarding a user of a network; wherein the set of data is a first set of data that is collected over a first duration of time; receiving a second set of data that is collected over a second duration of time, wherein the first duration of time is shorter than the second duration of time (see col. 6, lines 49-52); assessing a risk level of the user harming the network based on the second set of data, wherein the second duration of time is sufficient to collect historical data regarding past malicious activities of the user (see col. 6, lines 7-52 and col. 11, lines 49-53); assessing a current alert level based on the first set of data, wherein the first duration of time is of a length appropriate for assessing current activities of the user (see col. 16, lines 20-27);

automatically deciding on a course of action based on the set of data, wherein the course of action may be adverse to the user although the set of data is insufficient to establish whether the user is performing a malicious action; and sending signals to one or more network elements in the network to implement the decision (see col. 6, line 1 – col. 7, line 15).

In respect to claim 2, Proctor the system of claim 1, wherein the set of data includes at least one or more alerts related to the user (see col. 7, lines 5-15).

In respect to claim 3, Proctor discloses the system of claim 1, wherein the signals include multiple alerts generated by multiple users; and the system further comprising sequences of instructions for correlating the multiple alerts to the multiple users (see col. 7, lines 15-26).

In respect to claim 6, Proctor discloses the system of claim 1, further comprising sequences of instructions for performing the steps of: receiving signals related to an external source including at least an alert assessment relevant to the network as a whole; and creating and storing a current alert level value based on the alert assessment (see col. 6, line 25-col. 7, line 40).

In respect to claim 7, Proctor discloses the system of claim 1, further comprising sequences of instructions for performing the steps of:

receiving signals carrying performance information related to a health level of the network; and determining the course of action based at least in part on the set of data and the performance information (see col. 1, line 65-col. 2, line 50 and col. 6, line 49-col. 7, line 40).

In respect to claim 8, Proctor discloses the system of claim 1 further comprising:
a plurality of routers for routing information sent by users and servers to a variety of destinations;

a subscriber management system for managing a network; a controller for executing the sequences of instructions; a network element for generating input for the set of data; and sequences of instructions for sending signals to the network elements (see col. 15, line 25-col. 17, line 10).

In respect to claim 9, Proctor discloses a computer-readable medium carrying one or more sequences of instructions for providing policy-based network security management, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of (see Abstract):

receiving signals carrying network performance information regarding health of a network and resource performance information regarding health of resources used by a network (see col. 1, line 65-col. 2, line 6 and 47-50); assessing a health level based on the network performance information and the resource performance information; and

Art Unit: 2134

sending signals carrying information affecting use of the network based on at least the health level (see Fig. 10 and 11, col. 3-4-18 and col. 16, lines 20-26).

In respect to claim 10, Proctor discloses a computer-readable medium as recited in claim 9, further comprising the steps of:

receiving signals related to one or more alerts; associating with a user at least the one or more alerts within a current alert dataset that establishes a current alert level for the user (see col. 6, line 52-col. 7, line 15).

In respect to claim 11, Proctor discloses a computer-readable medium as recited in claim 9, further comprising the step of establishing a user alert (see col. 7, lines 5-15).

In respect to claim 12, Proctor discloses the computer-readable medium as recited in claim 9, further comprising the steps of: receiving signals related to one or more alerts; associating with a user at least the one or more alerts within a historical dataset of alert related information that establishes a user risk level for the user (see col. 6, line 52-col. 7, line 15).

In respect to claim 13, Proctor discloses the computer-readable medium as recited in claim 9, wherein the step of sending signals further comprises the steps of: deciding on a course of action based on at least a user risk level, a current alert level, and the health level, wherein the information effecting the user of the network is based at least

the course of action (see col. 6, line 1 – col. 7, line 15, col. 16, lines 26-27).

In respect to claim 14, Proctor discloses the computer-readable medium as recited in claim 13, wherein the deciding step include at least: determining the user risk level and determining a alert level, wherein the information affecting the user of the network is based on at least the user risk level, the current alert level and the health level (see col. 6, lines 7-52 and col. 11, lines 49-53 and col. 16, lines 26-27)

In respect to claim 15, the claimed limitation is similar to claim 9. Therefore, claim 15 is rejected based on the similar rationale.

In respect to claims 16-18 and 21-24, the claimed limitations are similar to claims 1-7 and 9. Therefore, claims 16-18 and 21-24 are rejected based on the similar rationale.

In respect to claim 25, Proctor discloses the method of claim 23, wherein the sending step further comprising the steps of :

Deciding on a course of action based on *at least* a user risk level, a current alert level, and the overall network health level, and the information affecting the use of the network includes at least information form carrying out the course of action ((see col. 6, line 52-col. 7, line 25).

Art Unit: 2134

In respect to claim 26, Protor discloses the method of claim 25, wherein the deciding step include at least the steps of:

Determining the user risk level; determining the current alert level; and determining the overall network health level; wherein the information affecting the user of the network is based on at least the user risk level, the current alert level and the overall network health level (see (see col. 6, lines 7-52 and col. 11, lines 49-53 and col. 16, lines 26-27).

In respect to claim 30, the claimed limitation is an apparatus claim that is substantially similar to computer-readable medium claim 9. Therefore, claim 9 is rejected based on the similar rationale.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Protor (U.S. Patent No. 6,530,024).

In respect to claims 27-28, Protor discloses a method of policy network security management, comprising the computer-implemented steps of:

Collecting network performance statistics related to an overall health of a network and individual performance statistics of one or more individual units of the network, the collecting being performed by a performance management system; Sending the network performance statistics to a controller for analysis; Computing an overall health state based on the network performance statistics and the individual performance statistics, using the controller; Reading external alert data from an external alert source, using the controller; collecting security event data from the network; Sending the security event data from the network (see col. 3, lines 19-35 and col. 13, lines 35-59);

Sending the security event data to a fault management system;

Calculating an alert state based on the security event data (see col. 16, lines 19-26); Obtaining user information from a subscriber management system; Reading external user risk data from an external user risk source into the controller; Calculating a user risk state based on the correlated security event data and the external user risk data, using the controller (see col. 5, lines 30-44 and col. 6, lines 8-20);

Calculating a decision regarding whether to take corrective action based on the overall health state, the alert state, and the user risk state, using the controller; Sending the decision from the controller to the subscriber management system; and sending directive, related to the decision, from the subscriber management system to the network (see Fig. 2 and Fig. 12, col. 5, line 63-col. 6, line 48, col. 12, lines 32-67 and col. 16, line 19-26);

Protor Correlating the security event data with the user information to form correlated security event data (see col. 6, lines 8-20) but does not disclose using the

Art Unit: 2134

fault management system for checking for duplications in the security event data, and deduplicating duplicate security events in the security event data. However, removing duplicating data from database is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to removing duplication from collected data taught by Protor to check for error of duplicate data and to removed duplication before data assessment to ensure integrity of the data analyses.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Art Unit: 2134

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-3962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Examiner: Tongoc Tran
Art Unit: 2134

May 9, 2006


JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER